Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 58 (2015) 544 – 551
Procedia Computer Science

Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Secure Communication over Trellis using Fundamental Cut-set and Fundamental Circuits

R Selvakumar[a,*], Pavan Kumar C[a], Raghunadh K Bhattar[b]

[a]*School of Advanced Sciences, VIT University, Vellore - 632014, India*
[b]*Space Applications Center, ISRO, Ahmedabad, India*

Abstract

Trellis representation of codes helps in analyzing and understanding the nature of the codes. Trellis has the connected graph nature where all paths from the 'root' vertex to 'goal' vertex forms the codewords. Efficient encoding and decoding algorithms are existing for communication over trellis. In the conventional communication system, Trellis is constructed for the encoded message at the sender and the algorithm such as Viterbi is used to decode the encoded message at the receiver. Any receiver with such decoding mechanism can be able to decode the message, which gives the chance for the intruder to get the message making the communication insecure. In this paper we propose a reliable and secure communication system which provides reliability by the Error Correction Techniques and Security by the graph based Cryptosystem. Using such system intruder's access to the information can be avoided and also if any errors occurred during transmission over noisy channel can be corrected. We have used Kernel codes and it's Trellis representation to demonstrate the construction of reliable and secure cryptosystem.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Keywords: Reliability; Security; Trellis; Fundamental Cut-sets; Fundamental Circuits

1. Introduction

Forney introduced 'Trellis' to represent linear block codes[1]. Kschischang and Sorokine[1] defined, Trellis for a block code C of length n is an edge labeled directed graph with a distinguished "root" vertex having in-degree zero and a distinguished "goal" vertex having out-degree zero, and with the following properties:

1. all vertices can be reached from the root;
2. the goal can be reached from all vertices;
3. the number of edges traversed in passing from the root to the goal along any path is n; and

* Corresponding author. Tel.: +91-416-2202850 ; fax: +91-416-2243092.
E-mail address: rselvakumar@vit.ac.in, sriviselva@yahoo.com

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.071

4. the set of n-tuples obtained by 'reading off' the edge labels encountered in traversing all paths from the root to the goal is C.

Bahl et. al.[2] constructed trellis for binary linear block codes in the context of finite size Markov chains with finite states and transitions. Further, Wolf[3]showed the possibility of decoding of linear binary block codes constructed by Bahl et. al.[2] using Viterbi algorithm. Various researchers have proposed alternate construction techniques for Trellis. The properties such as Observability, Controllability and minimal trellises for codes have been studied with emphasis on Algebra and Graph theory as well[1,4,5].

In the traditional communication system, the message is encoded at the sender and decoded at the receiver side. Trellis is constructed for the encoded message and the algorithm such as Viterbi is used to decode the encoded message at the sender and receiver respectively. Any receiver with such decoding mechanism can be able to decode the message, which gives the chance for the intruder to get the message making the communication insecure.

To overcome the problem of insecure or unauthorized decoding of message over trellis, in this paper, by considering the connected graph nature of Trellis we propose a model for reliable and secure communication in which the message is encoded and encrypted at the sender side and the same will be decrypted and decoded at the receiver side. The cryptosystem designed works as a private key cryptosystem, as same set of keys is used at sender and receiver for encryption and decryption. Forward error correction algorithms provides reliability for communication over Trellis and our proposed method over Trellis provides secure communication as the receivers with pre-shared 'keys' can only decrypt the message even though the message is being received by multiple receivers.

Section 2 of the paper deals with construction of Trellis and basic terminologies required for the proposed method. Section 3, discusses the proposed scheme helpful in achieving reliable and secure communication over Trellis. It is showed that fundamental cut-set and fundamental circuits can be used for secure communication[6]. In section 4, implementation example of proposed scheme is discussed. Section 5 deals with conclusions.

2. Codes, Trellis, Spanning Trees

We have used a class of group codes called Kernel codes[7] to demonstrate reliable and secure communication system. The proposed system can be built over any Trellis representation of codes.

Kernel Codes are a class of group codes defined over finite groups and finite length codes are constructed using such codes. Kernel codes and its system property such as controllability is discussed in[7] and its application to unconventional DNA construction is discussed in[8].

2.1. Kernel Codes

Kernel codes are obtained by defining Homomorphisms from a set of finite groups to Abelian Group.
Construction is as follows:

Let G_1, G_2, G_3, ... G_n be groups and S be an abelian Group. The Kernel of Homomorphism is defined as $\mu(g_1, g_2, g_3, ..., g_n) = \mu_1(g_1)\mu_2(g_2)\mu_3(g_3)...\mu_n(g_n)$ where, μ_i is a homomorphism from $G_i \rightarrow S$, $i = 1, 2, 3, ..., n$

Homomorphism mapped to identity element of Abelian Group called as Kernel of Homomorphism. These homomorphisms can be defined as required to applications either as binary or non-binary. Algorithm 1 describes the procedure to construct Kernel codes K.

2.2. Trellis

Trellis can be constructed for the Kernel codes using any Trellis construction procedure. Algorithm 2 describes the procedure to construct trellis for a group code. Trellis consists of labeled edges from state v_i to v_{i+1} with a label where v_i is the present state and v_{i+1} is the next state. Triplet (v_i,a,v_{i+1}) is used to indicate trellis edge from present state v_i to next state v_{i+1} with label a, algorithm 2 generates such triplets from the group of Kernel codes $K = \{k_1, k_2, ..., k_m\}$ and Trellis graph will be constructed accordingly. The trellis path from "root" vertex to "goal" vertex in the Trellis is a valid codeword of code C and the number of such paths is equal to the number of codewords possible for the code C.

Algorithm 1 Kernel Codes K

for $i = 1$ *to* n **do**
  μ_i = *select values suitable for channel*
end for
Compute set C of Cartesian product $(g_1, g_2, g_3, ..., g_n)$ of Finite Groups G_1,G_2,G_3,...,G_n using any algorithm
for $i = 1$ *to* n **do** ▷ On set C of Cartesian products
  if $\mu_1(g_1)\mu_2(g_2)\mu_3(g_3)...\mu_n(g_n) = 0$ **then**
    add to set K
    return K
  end if
end for

Algorithm 2 Trellis Triplets

for $i = 1$ *to* m **do** ▷ On set of Kernel Codes K
  $s_i = 0.$ ▷ Initial condition for root vertex
  for $j = 1$ *to* n **do**
    $s_j = s_i \times a$
    $E_{ij} \leftarrow (s_i, a, s_j)$ ▷ Triplet for Trellis edge
  end for
end for

2.3. Spanning Trees

A tree T is said to be a spanning tree of a connected graph G if T is sub graph of G and T contains all vertices of G[9]. Few spanning trees of Trellis obtained is shown in figure 4.

In our proposed method we use only the spanning trees having valid codewords so that we can get back the trellis graph by combining all the spanning trees based on their vertex labeling.

2.4. Fundamental Circuits and Fundamental Cut-set

2.4.1. Fundamental Cut-sets

Consider any branch b in a spanning tree T of a connected graph G, branch {b} partitions all vertices of spanning tree into two disjoint sets - one at each end of b. Consider the same partition of vertices in G and the cut set S in G corresponding to this partition, the cut set S will contain only one branch b of T and the rest of edges in S are chords of T which are present in G. Such a cut-set S containing exactly one branch of a tree T and remaining branches from G is called a fundamental cut-set with respect to T[9]. Such a cut-set S will have meaning only with respect to that particular spanning tree.

2.4.2. Fundamental Circuits

Consider a spanning tree T in a given connected graph G. Let c_i be a chord with respect to T, and let the fundamental circuit made by c_i be called C, consisting of k branches $b_1, b_2, ..., b_k$ in addition to the chord c_i that is C = { $c_i, b_1, b_2, ..., b_k$ } is a fundamental circuit with respect to T[9].

For example consider the spanning tree in figure 4(f) of connected graph in figure 3, consider the edge connecting D and F it partitions all vertices of spanning tree into two disjoint sets {B, A, C, D} and {F, E}. The cut-set S will have {h, g, f, i} where 'h' is a branch in spanning tree and the remaining edges are from graph G. Set S forms the fundamental cut-set with respect to the spanning tree in figure 4(f). Similarly, consider edge cut-set S of G, adding of chord 'e' to the spanning forms a fundamental circuit.

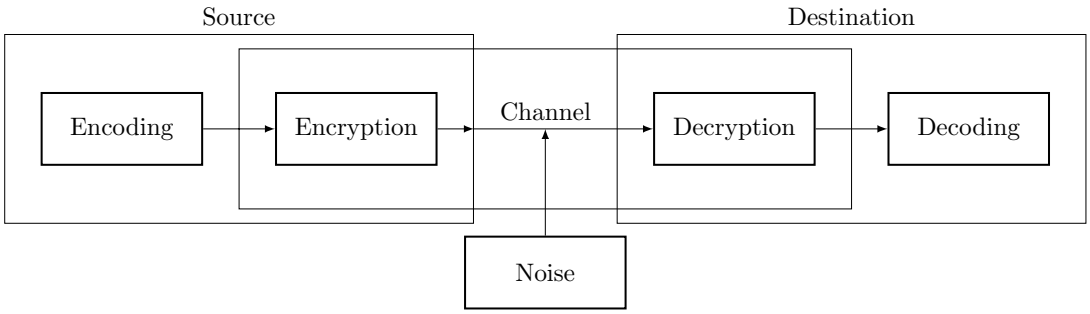


Fig. 1. Reliable and Secure Communication System

3. Reliable and Secure Communication System

Figure 1 describes reliable and secure communication system in which message is encoded and encrypted at the sender side and decrypted and decoded at the receiver side respectively to get the original message.

Message encoding can be done using any of the coding techniques and trellis is constructed for the encoded message. Further, encryption algorithms based on graph nature are used to encrypt the encoded message. Similarly, at the receiver, the received message is decrypted first and further decoded to get original message.

The following fundamental circuits and fundamental cut-sets theorems[9] is used in establishing cryptosystem.

Theorem 1. *With respect to a given spanning tree T, a branch b_i that determines the fundamental cut-set S is contained in every fundamental circuit associated with the chords in S and in no others.*

Theorem 2. *With respect to a given spanning tree T, a chord c_i that determines the fundamental circuit C occurs in every fundamental cut-set associated with the branches in C and in no others.*

In the proposed method, Trellis obtained for the encoded message is converted into an equivalent labeled graph with renaming of the edges and vertices. Spanning trees are generated for the graph such that each spanning tree has a valid codeword. At the sender side, Theorem 1 is used to generate cut-set which acts as a key at the receiver to decrypt. At the receiver side, from the cut-set and spanning tree received fundamental circuits are constructed as in Theorem 2. All the circuits thus obtained are compared and in all circuits only one edge will be common which makes the edge authentic. Further, the labeled graph is renamed with original values assigned at the sender. Thus, getting back the actual trellis.

Further, Trellis is decoded using algorithm like Viterbi to get the original message which was encoded at sender. If the noise is added in the channel, combining of spanning trees at the receiver ensures that original message is not lost even though an edge is deleted from the graph as a particular edge will be present in other spanning trees as well. But such deletion doesn't affect the system as Viterbi like algorithm uses Hamming distance property to effectively decode the message. Only the path with less weight from 'root' vertex to 'goal' vertex is considered to decode.

Table 1 summarizes the procedure in establishing the reliable and secure communication system at the sender and receiver respectively.

4. Example

Let Z be the group of Integers. Kenrel codes and trellis are constructed from algorithms mentioned in algorithm 1 and algorithm 2 respectively.

Consider $Z_3 \times Z_2 \times Z_3 \rightarrow Z_2$ be finite groups with homomorphisms μ_i defined as $\mu_1(0) = 0, \mu_1(1) = 1, \mu_1(2) = 1, \mu_2(0) = 0, \mu_2(1) = 1, \mu_3(0) = 0, \mu_3(1) = 1, \mu_3(2) = 0$.

The Cartesian products of above defined finite groups are {000, 001, 002, 010, 011, 012, 100, 101, 102, 110, 111, 112, 113, 201, 202, 210, 211, 212}

By defined values of homomorphisms and computing zero homomorphisms as mentioned in figure 1, we obtain {000, 002, 011, 101, 110, 112, 201, 210, 212} as Kernel codes.

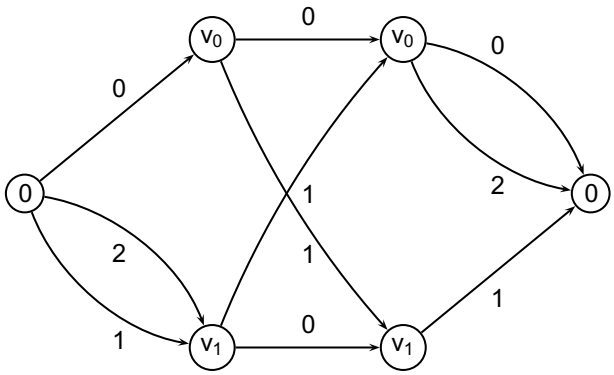


Fig. 2. Trellis of the Kernel codes

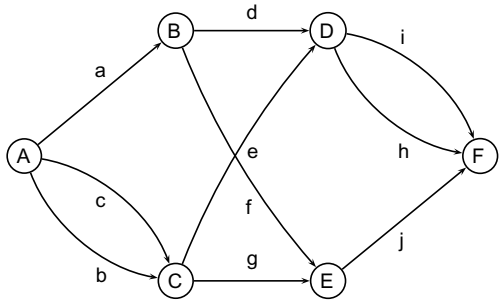


Fig. 3. Labeled graph of the Trellis

Table 1. Summary of procedures at Sender and Receiver

Sender	Receiver
1. Encodes the message using any coding technique 2. Trellis is constructed for the Encoded message 3. Equivalent labeled graph is constructed for the Trellis graph to avoid name ambiguity 4. Spanning trees are constructed for the labeled graph each having valid codewrods 5. Edge cut is made and spanning tree and corresponding cut-set is sent to the receiver. Cut-set acts as a key.	
	1. Construct the fundamental circuits from the spanning tree and the cut-set 2. Compare all the circuits formed. 3. Edge common in all the circuits will be unique and it proves the authenticity of edge. 4. All spanning trees received are combined after constructing fundmantal circuits and obtaining unique edge 5. Combined graph will be the labeled graph. By substituting the actual values the graph is further decoded by graph algorithms like Viterbi to obtain the actual message.

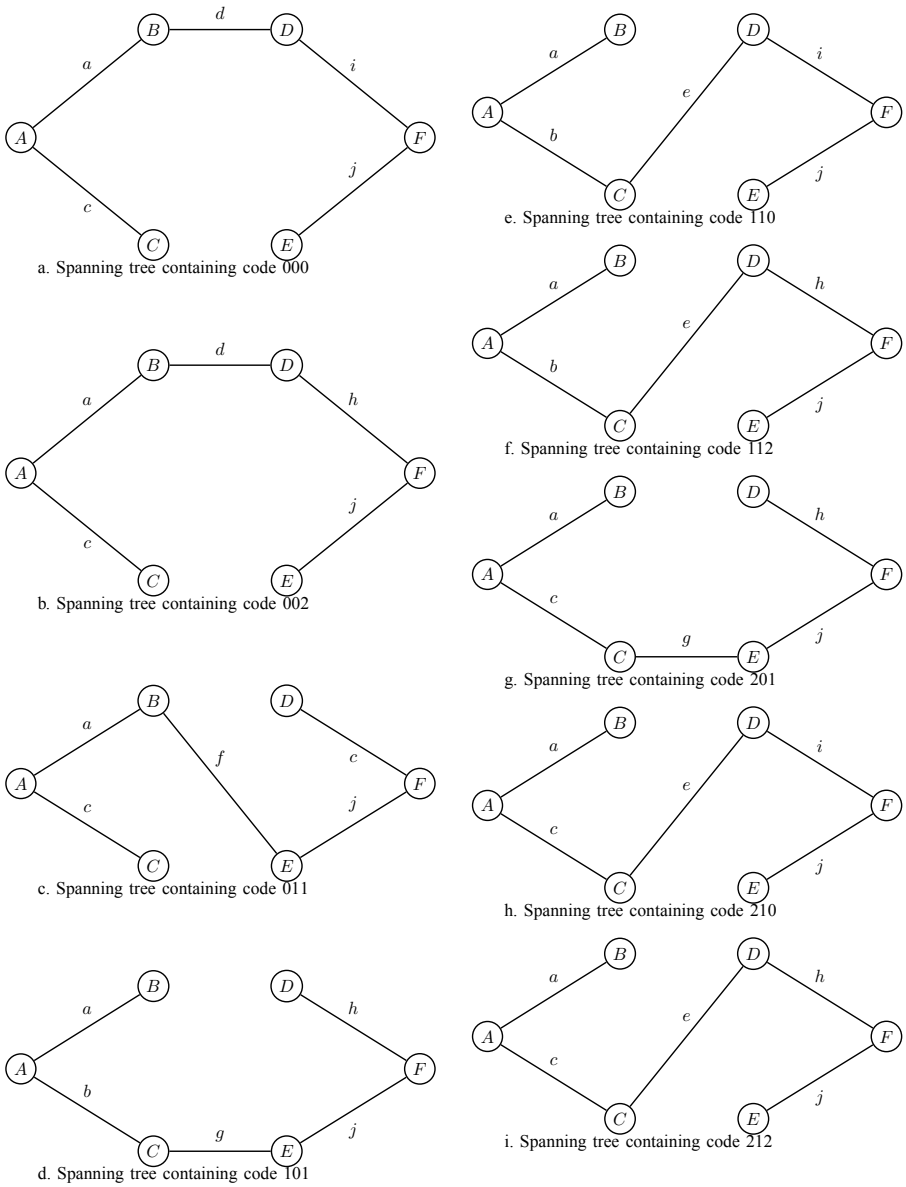


Fig. 4. Spanning Trees of labeled graph of Figure 3 having valid codewords

Constructing trellis triplets as mentioned in algorithm 2, we obtain trellis graph of Kernel Codes. The minimal trellis will be constructed for trellis by removing all edges which are not having direct connection from ”root” vertex to ”goal” vertex, the minimal trellis for the above Kernel code is given in figure 2.

Only a limited number of spanning trees are selected from connected graph of figure 3, such that each spanning tree has a valid codeword in it from ”root” vertex to ”goal” vertex.

Fundamental cut-set can be obtained by selecting any arbitrary edge of spanning tree. Consider the spanning tree in figure 4(f), it has the valid codeword 112, perform the cut over the edge ’h’ as shown in figure 5. Cut-set formed will be {h, i, g, f} in which only ’h’ is the branch of spanning tree and remaining are the edges of the connected graph in figure 5. From the cut-set, fundamental circuits are constructed at receiver side as shown in figure 6. In all

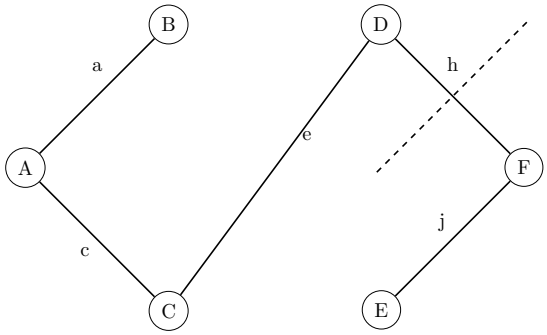
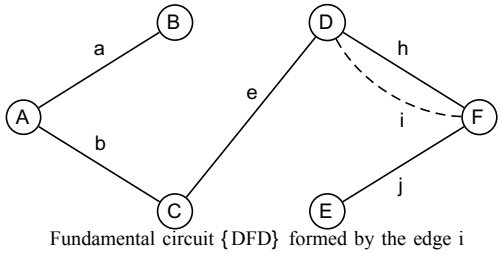
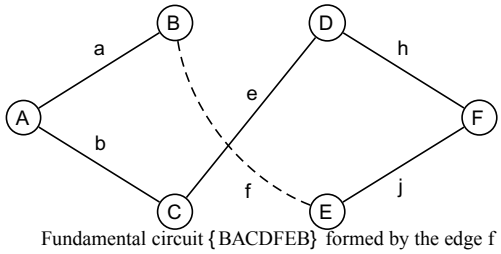


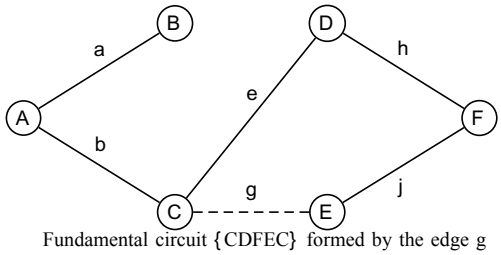
Fig. 5. Cut over edge h in spanning tree



Fundamental circuit {DFD} formed by the edge i



Fundamental circuit {BACDFEB} formed by the edge f



Fundamental circuit {CDFEC} formed by the edge g

Fig. 6. Fundamental circuits by connecting cut-set edges

three circuits, {DFD, BACDFEB, CDFEC}, the edge 'h' is common which makes the edge authentic. Thus, verified spanning trees will be combined again in order to obtain the connected graph as in figure 3.

Viterbi algorithm or any similar algorithm can be used to decode the trellis based on Hamming distance and get the message path in the trellis based with minimum hamming weights from 'root' vertex to 'goal' vertex.

5. Conclusions

To overcome the drawback of unauthorized access to information in the traditional communication systems and to correct the possible errors in communication over transmitting channel, we proposed a reliable and secure communication system using the graph nature of Trellis. With the help of Kernel codes and its trellis, we have showed the construction of cryptosystem over trellis where in fundamental cut-set and fundamental circuit are used to encrypt and decrypt the message at the sender and receiver respectively. Building cryptosystem over Trellis have been a novel approach and not been studied in the literature previously. Further, the fundamental cut-set and fundamental circuits can also be used independently or in combination to build such cryptosystems in addition to the existing crypto standards.

Acknowledgements

This work was partially supported by Indian Space Research Organization through its grants ISRO/RES/3/645/2014-15.

References

1. Kschischang, F.R., Sorokine, V.. On the trellis structure of block codes. *Information Theory, IEEE Transactions on* 1995;**41**(6):1924–1937.
2. Bahl, L., Cocke, J., Jelinek, F., Raviv, J.. Optimal decoding of linear codes for minimizing symbol error rate (corresp.). *Information Theory, IEEE Transactions on* 1974;**20**(2):284–287.
3. Wolf, J.K.. Efficient maximum likelihood decoding of linear block codes using a trellis. *Information Theory, IEEE Transactions on* 1978; **24**(1):76–80.
4. Muder, D.J.. Minimal trellises for block codes. *Information Theory, IEEE Transactions on* 1988;**34**(5):1049–1053.
5. Forney Jr, G.D.. Codes on graphs: normal realizations. *Information Theory, IEEE Transactions on* 2001;**47**(2):520–548.
6. Selvakumar, R., Gupta, N.. Fundamental circuits and cut-sets used in cryptography. *Journal of Discrete Mathematical Sciences and Cryptography* 2012;**15**(4-5):287–301.
7. Selvakumar, R., Balasubramani, P.. Kernel code and its controllability. *Journal of Discrete Mathematical Sciences and Cryptography* 2004; **7**(1):97–101.
8. Selvakumar, R.. Unconventional construction of dna codes: Group homomorphism. *Journal of Discrete Mathematical Sciences and Cryptography* 2014;**17**(3):227–237.
9. Deo, N.. *Graph theory with applications to engineering and computer science*. PHI Learning Pvt. Ltd.; 2004.